2.   Rejection of Claims 11 and 12 Under 35 USC §102(e) in view of U.S. Patent No. 6,185,603 (Henderson)

This rejection is respectfully traversed on the grounds that the Henderson patent fails to disclose or suggest an electronic mail system in which presentation of information contained in an electronic mail *wrapper* is controlled by a viewer applet on the *recipient's* computer. Instead, the viewer applet ("Display Application 16") of Henderson merely displays text messages extracted by a mail server from subject lines in the message, in response to a code inserted into the subject line by the user and recognized by the server.

Claim 11 now recites that the viewer applet installed on the recipient's computer decodes selected control options, searches for appropriate fields in the message wrapper, *and* carries out the desired wrapper controls in response to the control options, before presenting the modified electronic mail package to the recipient. These functions of the viewer applet are described in lines 3-12 on page 44 of the original specification, and illustrated in Fig. 15.

There is no disclosure in Henderson that the viewer applet 16 manipulates or controls an electronic mail wrapper in the manner now recited in claim 11. Instead, the sender inserts a special code in the subject line of an electronic mail message, followed by a message. The server then sends the message extracted from the subject line for display on the recipient's computer. In each of the examples given in the Henderson patent, the extracted messages are text messages from the sender to the recipient. For example, the sender might insert the message "Alert-The 10 am meeting is canceled!" after the control code in the subject header (col 7, line 10) of Henderson, so that this message is displayed by the Display Application 16, without the need for the recipient to follow usual mail opening and reading procedures. In contrast, the claimed viewer applet actually *controls* the display of wrapper information, such as the identity of the sender and the time the message was sent.

While the instant messaging system of Henderson involves the "subject" line included in an electronic mail wrapper, it does not involve using a viewer applet to control a manner in

2

which information items in the electronic mail wrapper are presented to the recipient, as claimed. Instead, Henderson merely provides a way to embed message text in the header, so that the message can be conveniently displayed. As a result, it is respectfully submitted that the Henderson patent does not anticipate the claimed invention, and withdrawal of the rejection of claims 11 and 12 is respectfully requested.

3. Rejection of Claims 14 Under 35 USC §103(a) in view of U.S. Patent Nos. 6,324,569 (Ogilvie)

This rejection is respectfully traversed on the grounds that the Ogilvie patent fails to disclose or suggest encrypting a message so that a viewer is prevented from viewing message *wrapper* information unless controls on display of the information are implemented, as recited in claim 14. Instead, Ogilvie permits an e-mail to be freely viewed, and merely provides for expiration of an e-mail to save the recipient the trouble of deleting it if the recipient is not interested in the e-mail.

Like the present invention, the Ogilvie patent discloses systems and methods for enabling an originator to designate an expiration date for e-mail. However, the reason that Ogilvie includes the expiration date is so that the recipient does not have to bother with deletion of the e-mail. The recipient is free to over-ride the expiration date and continue viewing the e-mail. In contrast, the claimed invention seeks to provide absolute originator-control of the expiration date, so that it is impossible for the recipient to prevent expiration. This is accomplished by encrypting the message so that it can only be read by a viewer applet arranged to implement the originator-controls.

According to the aspect of the invention recited in claim 14, the originator-control in question is control of message wrapper information display. The message wrapper includes information concerning the sender and/or origination of the message, including sender identification and time/date of sending. Because this information is encrypted, it can only be

displayed by a viewer applet capable of decrypting the information, thereby <u>requiring</u> viewing through an applet that can be controlled by the originator.

Ogilvie does not anywhere mention the type of encryption that enables originator or sender control of message, or message wrapper, viewing. Furthermore, Ogilvie does not need such encryption since Ogilvie's controls are for the convenience of the recipient, with the recipient preferably being given the option of over-riding the control. This makes sense since Ogilvie is designed to make spam more recipient friendly, *and it is to the sender's advantage in such cases if the recipient does desire to over-ride a control and keep the message in question.*

The passages cited by the Examiner as disclosing message encryption and message *wrapper* control, col. 5, lines 52-54 and col. 16, lines 8-13) do not appear to include any such teachings. Col. 5, lines 52-54 merely point out that the removal code may be embedded in the recipient's browser or email reception program, so that the recipient does not need to actively delete the message if he/she does not wish to save it. Col. 6, lines 8-13 describe the option of deleting the message automatically after a predetermined period, such as 24 hours after receipt. Nowhere do these passages suggest encryption of the message, much less control of information in the email *wrapper* as claimed. Since Ogilvie is simply concerned with convenience, and not with *preventing* a recipient from keeping a message longer than the designated expiration date, there is no need for Ogilvie to encrypt messages, or the message wrapper, as claimed.

Because Ogilvie fails to disclose or suggest all elements recited in claim 14, withdrawal of the rejection under 35 USC §103(a) is respectfully requested.

4. <u>Rejection of Claims 1-10 Under 35 USC §103(a) in view of U.S. Patent No. 5,958,005 (Thorne) and Netscape 2 Simplified ("Netscape")</u>

This rejection is respectfully traversed on the grounds that the Thorne patent and the Netscape publication fail to disclose or suggest an arrangement in which electronic mail controls are implemented by having the electronic mail creation program *divert* an electronic mail

4

message to a central (proxy) server, which implements the controls upon forwarding of the message to the destination address, as claimed in claim 1.

While the Netscape publication teaches a menu that permits modification of a destination address input by the user, the Netscape publication fails to disclose or suggest that the e-mail program substitute a destination address for the one entered by the user in order to divert the message to a proxy server that ultimately forwards the message to the selected destination address. Instead, the passage referred to by the Examiner concerns the manner in which the user enters the destination address, and not the substitution of a central server address for the destination address typed in by the user. As explained in item 9 on page 112 of the Netscape publication, the sender should:

> *Type the address of the computer that receives your messages and then press TAB on your keyboard.*

This passage simply states that the user should enter the address of the recipient if the user wants to send a message to the recipient. It does not tell the user to also enter the address of a central server, much less suggest to the ordinary artisan that the program should substitute the address of the central server for the one typed in by the user.
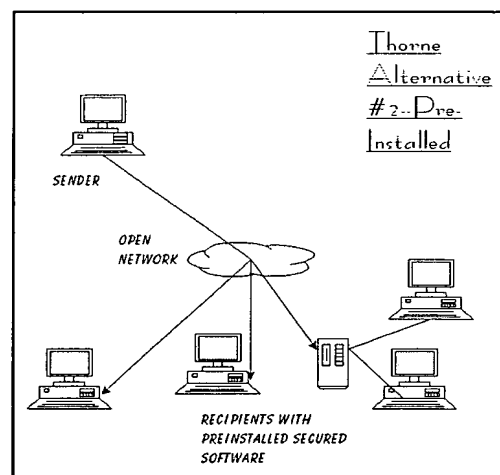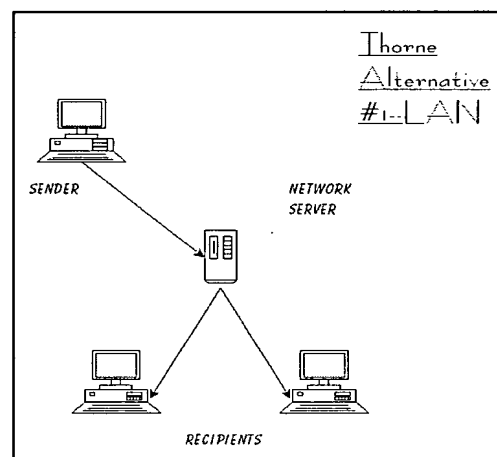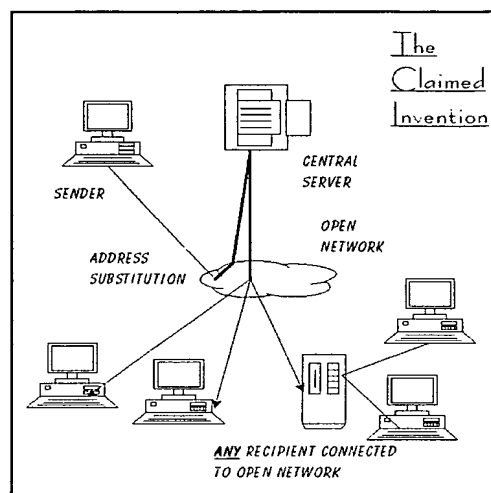
Since Thorne also does not suggest a proxy mail server for achieving the controls disclosed therein, and since the Netscape publication does not suggest the substitution necessary to carry out the proxy function, it is respectfully submitted that one of ordinary skill in the art could not have combined the teachings of Thorne and Netscape to achieve the claimed invention.

It is true that Thorne modifies an electronic mail creation program to enable controls to be set. However, Thorne achieves the controls in a manner that is contrary to that presently recited in claim 1. In Thorne, the destination address input by the user is not changed by the mail creation program, and the only way that the controls can be implemented is if the sender's computer is connected to a LAN server arranged to implement or enforce the controls, if a server in the normal route taken to the destination address has been appropriately modified, or if the

recipient's viewer is already arranged to implement the controls set by the sender's electronic mail creation program. Since Netscape's program simply permits the user to change destination addresses, and does not involve swapping or substitution of addresses in a way that would permit use of a proxy to control handling by a recipient, Netscape could not have suggested modification of Thorne's control arrangement to achieve such substitution.

The Claimed Invention

CENTRAL SERVER

SENDER

OPEN NETWORK

ADDRESS SUBSTITUTION

ANY RECIPIENT CONNECTED TO OPEN NETWORK

In the claimed invention, it is the electronic mail program that selects the proxy server address, based on the input of controls by the user. The user simply enters the ultimate destination address, and the electronic mail program takes care of the address swapping, so that the process is transparent to the user. Mere changing of destination addresses by the user, as in the Netscape system, will not accomplish any objectives of the invention and will not result in the claimed address swapping since all that will happen is that the ultimate destination address will be changed.

Thorne Alternative #1—LAN

SENDER

NETWORK SERVER

RECIPIENTS

Thus, while the Thorne patent does disclose a system that enables control options including message expiration date to be set by the sender using a "template" similar to the claimed "window," the control options are either implemented by causing "*each recipient computer or processor to respond to the commands created by completion of the template,*" or

Thorne Alternative #2—Pre-Installed

SENDER

OPEN NETWORK

RECIPIENTS WITH PREINSTALLED SECURED SOFTWARE

by limiting the recipient to electronic mail applications that run from a local server. Neither of these alternatives involves a <u>proxy</u> server such as the claimed central mail server, and neither requires the sender's electronic mail program to substitute an input destination address for the address of the proxy server.

The operation of the software recited in claims 1-10 is illustrated in Figs. 1-3 and 6 of the present application. Normally, the software sends a message to a recipient by inserting the recipient's address into a destination header, and sending the electronic mail package to a local server, which routes the message through one or more nodes to the recipient. If controls are desired, however, the mail creation software actually **substitutes** the central server's address for the original destination address (for example by changing entry's in the software's address book), inserts the substituted central server's address into the destination header, and sends the electronic mail message through normal electronic mail channels to the central mail server, which implements the controls without affecting normal mail handling procedures or routing protocols. The central mail server ensures that the controls are implemented by, for example, encrypting the message and streaming it to a secured viewer applet on the recipient's computer and, if the recipient's computer does not already include a secured viewer applet, supplying the viewer applet to the recipient's computer.

While other claims of the present application are directed to the manner in which the central server implements desired controls, claims 1-10 are concerned solely with the sender's electronic mail creation software, and in particular with the feature <u>in the software</u> that enables the controls to be implemented by the central server, namely the feature in which the sender's software *diverts* mail to the proxy server. It is this feature that enables the controls to be efficiently implemented over an open network, without limiting the application to a LAN or to recipients having pre-installed applications that will, as described in col. 8, lines 46-52 of Thorne, *"operate with the system."* Neither Thorne nor Netscape ever contemplates diverting electronic mail to a central server over an open network, as claimed, with Netscape lacking any sort of controls and Thorne only contemplating an arrangement in which the computers are all on the

7

same LAN, or in which electronic mail is addressed solely to recipients having computers on which secured software has been pre-installed.

As a result of these differences, it is respectfully submitted that the electronic mail creation system and method recited in claims 1-10 is not only novel, but also represents an inventive step over the system and method described in the Thorne patent.

5.   Rejection of Claims 13, 15, 19, and 22 Under 35 USC §103(a) in view of U.S. Patent
      Nos. 6,185,603 (Henderson) and 6,324,569 (Ogilvie)

This rejection is respectfully traversed on the grounds that neither the Henderson patent nor the Ogilvie patent discloses or suggests encryption of an electronic mail message in order to control display of information in the wrapper, as discussed above.

Henderson merely displays plaintext messages extracted from a message header, the messages being designated by adding designators to the header without the need for encryption, while Ogilvie discloses a system that permits unwanted e-mails to be automatically deleted, but permits saving or viewing of the e-mails if the viewer so desires, and is not concerned with giving the *sender* control of message handling by encrypting the message.

Accordingly, neither Henderson nor Ogilvie, whether considered individually or in any reasonable combination, could possibly have suggested the claimed invention and therefore withdrawal of the rejection of claims 13, 15, 19, and 22 under 35 USC §103(a) is respectfully requested.

6.   Rejection of Claims 16-18 Under 35 USC §103(a) in view of U.S. Patent Nos. 6,185,603
      (Henderson), 6,324,569 (Ogilvie), and 6,005,945 (Whitehouse)

This rejection is respectfully traversed on the grounds that the Whitehouse patent concerns a system and method for dispensing postage for "snail mail" based on telephonic or web "millitransactions," rather than an electronic mail system.   Cited solely for its teachings concerning use of a session key encryption method rather for any particular teachings concerning

8

electronic mail, the Whitehouse patent, like the Henderson and Ogilvie patents, fails to disclose or suggest the claimed control of a message wrapper by encryption, whether or not a session key is used.

Furthermore, Whitehouse does not even remotely suggest periodic check-in by a viewer applet of the type claimed so that a server can check a clock in the recipient's computer, as recited in claim 18. Contrary to the Examiner's statement in the last sentence of item 11, claim 18 recites a distinct function that is not recited in claim 17 or disclosed in Whitehouse, namely clock checking. There is no need for the server of Whitehouse to check an e-mail recipient's clock, as claimed, since Whitehouse does not disclose enforced expiration of e-mails in a manner that would require such clock checking.

Because none of the applied references discloses or suggests the combination recited in claims 16-18, withdrawal of the rejection of claims 16-18 under 35 USC §103(a) is respectfully requested.

7.   Rejection of Claims 20 and 23 Under 35 USC §103(a) in view of U.S. Patent Nos. 6,185,603 (Henderson), 6,324,569 (Ogilvie), and 6,061,448 (Smith)

This rejection is respectfully traversed on the grounds that the Smith patent, like the Henderson and Ogilvie patents, fails to disclose or suggest control over electronic mail wrapper information display, as claimed, much less generation of a public-private key pair by a viewer applet that controls wrapper information display.
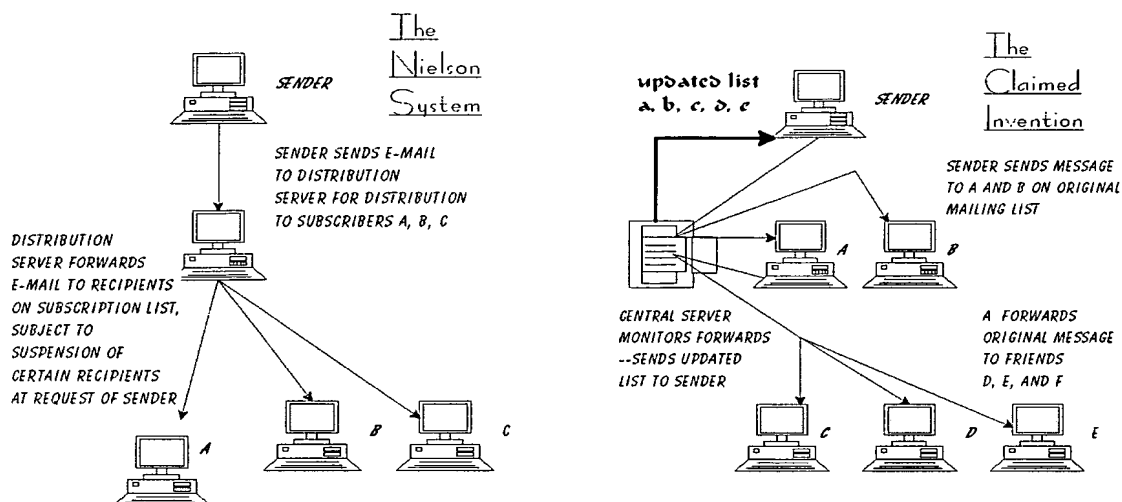
While it is known to use a recipient's public key to encrypt a message so that only the recipient can open it, using the recipient's private key, use of public key encryption for control of wrapper information display is not known, and not suggested by any of the references cited by the Examiner. As a result, withdrawal of the rejection of claims 20 and 23 under 35 USC §103(a) is respectfully requested.

8.   Rejection of Claims 25 and 28 Under 35 USC §103(a) in view of U.S. Patent Nos. 5,864,684 (Nielsen), 5,734,901 (Sidhu), and 6,167,435 (Druckenmiller)

This rejection is respectfully traversed on the grounds that:

a.   The Nielson patent merely discloses a system that enables an e-mail distribution server to suspend forwarding of e-mail to a selected subscriber for a predetermined period, and does not enable the sender to track forwarding of the e-mail by a recipient to additional recipients, as claimed;

b.   The system disclosed in the Sidhu patent merely enables an application program to record activities by an e-mail program, and does not even remotely suggest tracking of transactions by recipients of an e-mail that has already been sent, much less modification of a distribution server of the type disclosed by Nielson to perform such tracking; and

c.   The Druckenmiller patent discloses an opt-in procedure that enables a distribution server of the type disclosed by Nielson to up-date a subscription list and add persons on a mailing list to the subscription list, and also fails to disclose expansion of the mailing list to previously unknown persons who receive e-mails from persons on the original mailing list (and further to recipients of e-mails forwarded by the recipients of the original e-mails).

The Examiner acknowledges that Nielson fails to disclose "tracking all transactions involving an electronic mail message and using a record of at least a portion of the transactions to expand the electronic mail list." This feature is of course the point of the invention, because it allows electronic mail lists to be expanded based on determinations by recipients that the message would be of interest to parties not already on the list, *i.e.*, their friends, co-workers, or relatives. For example, a product brochure about camping equipment might be forwarded to a hundred persons. Of those hundred persons, ten might be interested in camping, and each one of those might forward the brochure to two other persons who they believe are interested in camping. Unlike na ordinary distribution server of the type disclosed by Nielsen, the claimed invention permits the sender to identify the twenty previously unknown persons identified by the

The
Nielson
System

SENDER

SENDER SENDS E-MAIL
TO DISTRIBUTION
SERVER FOR DISTRIBUTION
TO SUBSCRIBERS A, B, C

DISTRIBUTION
SERVER FORWARDS
E-MAIL TO RECIPIENTS
ON SUBSCRIPTION LIST,
SUBJECT TO
SUSPENSION OF
CERTAIN RECIPIENTS
AT REQUEST OF SENDER

A

B

C

updated list
a, b, c, d, e

SENDER

The
Claimed
Invention

SENDER SENDS MESSAGE
TO A AND B ON ORIGINAL
MAILING LIST

A

B

CENTRAL SERVER
MONITORS FORWARDS
--SENDS UPDATED
LIST TO SENDER

A FORWARDS
ORIGINAL MESSAGE
TO FRIENDS
D, E, AND F

C

D

E

recipients as being interested in camping, and add them to the mailing list so that future brochures can be sent to them. The system disclosed by Nielson has no such list-expanding effect, and the Sidhu and Druckenmiller patents do not suggest any way to modify the system of Nielson to achieve such an effect. While the ability to program a distribution server to suspend mailings to subscribers might avoid annoyance to certain recipients on the original list, it does not enable expansion of the list in the manner claimed.

The Sidhu patent merely enables an application program to communicate with an e-mail program. While this might involve recording transactions, it does not involve recording the transactions of *recipients* of the e-mail, and therefore could not possibly have suggested modification of the distribution server control of Nielson to provide such a record. The distribution server of Nielson in fact <u>cannot</u> provide such a record because, once the e-mail is sent by the distribution server, it is out of the control of the distribution server. As the Examiner is undoubtedly aware, once an e-mail is received by a conventional e-mail program, the recipient can send the e-mail anywhere without being tracked, whether it came from an individual or from a distribution server as part of a mass mailing.

11

The central server of the claimed invention is <u>not</u> analogous to the distribution server of Nielson, and also is not analogous to the application program of Sidhu. The difference is that, by <u>requiring</u> recipients to use viewer applets that proxy forwarded messages to the central server (if the recipient does not use the viewer applet, then the encrypted message cannot be read), the central server can in fact control <u>all</u> downstream distribution of forwarded e-mails. A distribution server of the type disclosed by Nielson is not capable of such downstream control, and therefor is not capable of tracking the e-mails in the manner claimed. The claimed invention is fundamentally different than, and has advantages not even remotely contemplated by, the system of Nielson, or the proposed combination of Nielson and Sidhu.

Furthermore, the inability of the distribution server of Nielson (or Nielsen in view of Sidhu) to track downstream forwarding of messages on the original mailing list is not remedied by Druckenmiller. The Druckenmiller patent merely prevents a person from being permanently added to a subscription list unless that person opts-in. In order to given an opportunity to opt-in to the <u>subscription</u> list, the address of that person must already be known to the sender, *i.e.*, the person must be on an original <u>mailing</u> list. Druckenmiller does not disclose or suggest expansion of the <u>mailing</u> list by tracking forwarding of the messages by persons on the original list, much less by tracking forwarding of messages by persons not on the original mailing list to whom the messages were forwarded by persons on the original mailing list.

In the system of Nielson, a distribution server stores e-mail distribution lists. When a sender wants to distribute the e-mail, the e-mail is sent to the distribution server, which then forwards the e-mail to persons on the distribution list, subject to certain suspension provisions. Once the e-mail is forwarded, the sender must wait for responses from recipients. Except for the suspension provisions, this is the conventional model for e-mail mass mailings. Nothing in either Sidhu or Druckenmiller suggests variation of this basic model. In contrast, the claimed invention provides for tracking of the e-mail from the recipient to all of the recipients friends and relatives to whom the *recipient decides* to forward the e-mail. Thus the list is <u>expanded,</u> utilizing the knowledge of the recipients, to persons who are not on the original mailing or distribution list.

While the central server of the invention may have the function of a distribution server, it is a distribution server that does not merely distribute, but actually tracks e-mails <u>after</u> distribution.

Furthermore, this tracking does not depend on the whether a recipient sends an opt-in message back to the distribution server as in Druckenmiller. In the claimed invention, recipients <u>must</u> opt-in in order to read the e-mail, which requires the positive step of acquiring and using the viewer applet, as described in Applicant's specification. Similarly, recipients of forwarded messages must also opt-in in order to read the e-mail. Thus, the list expands simply by the act of interested persons reading and forwarding the e-mail. Uninterested recipients of forwarded e-mails who choose not to read the e-mail, are not tracked and added to the original distribution list.

Nothing in any of the references cited by the Examiner even remotely suggests an e-mail list expander that expands a list beyond the original list provided to the distribution server by tracking every person interested enough to read and/or forward an e-mail. Accordingly, it is respectfully submitted that the rejection of claims 25 and 28-30 is improper and withdrawal of the rejection is respectfully requested.

10. <u>Rejection of Claims 25 and 28 Under 35 USC §103(a) in view of U.S. Patent Nos. 5,864,684 (Nielsen), 5,734,901 (Sidhu), 6,167,435 (Druckenmiller), 6,185,603 (Henderson), and 6,324,569 (Ogilvie)</u>

This rejection is respectfully traversed on the grounds that the Henderson and Ogilvie patents, like the Nielsen, Sidhu, and Druckenmiller patents, fails to disclose a system that tracks, or that even is capable of tracking, transactions involving an e-mail message *after* it has been forwarded by a distribution server, or other e-mail server, to persons on the *original* mailing list, so as to add the recipients of the forwarded e-mails to the original mailing list (as opposed to merely providing for suspension of mailings to particular subscribers (Nielsen); recording e-mail transactions on a particular computer (Sidhu); verifying whether the original recipients wish to opt-in or not (Druckenmiller); extracting alert messages from an e-mail subject line (Henderson);

and/or adding an automatic delete feature that automatically deletes and e-mail if the recipient is not interested (Ogilvie)).

As a result it is respectfully submitted that the rejection of claims 25 and 28 under 35 USC §103(a) is improper and should be withdrawn.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: September 19, 2002

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\beu\Pending I...P\L\LEONARD475112\a01.wpd

APPENDIX B
(Marked-Up Copy Of Amended Claims)

1. (Amended) Electronic mail control software, comprising:

means for opening a window arranged to enable a user of the electronic mail applications program to select

(i)   an original destination address to which an electronic mail message created using the electronic mail applications program is to be sent, and

(ii)   control options to be applied to [an] the electronic mail message [created using the electronic mail applications program]; and

means for [modifying] causing the electronic mail control software to substitute an address [to which the message is to be sent in order to direct the message to] of a central mail server [arranged] for the original destination address in order to divert said electronic mail message to a central mail server arranged to forward said electronic mail message to said original destination address and to implement said control options if one of said control options is selected.

6. (Amended) A method of adding lifespan and handling limitations to an electronic mail message, comprising the [steps] step of:

opening a window arranged to enable a user of the electronic mail applications program to select

(i)   an original destination address to which an electronic mail message created using the electronic mail application program is to be sent, and

(ii)   control options to be applied to [an] the electronic mail message [created using the electronic mail applications program; and],

[modifying] wherein, when one of said control options is selected by the user, the electronic mail applications program automatically substitutes an address [to which the message is to be sent in order to direct the message to] of a central mail server [arranged] for the original destination address in order to divert the electronic mail message to a central mail server arranged

23

to forward the electronic mail message to said original destination address and to implement said control options [if one of said control options is selected].

11. (Amended) An electronic mail system, comprising:

a first computer on which is installed message origination software and which is connected to a network capable of carrying an electronic mail wrapper that includes an electronic mail message;

at least one recipient computer also connected to said network; and

a viewer applet installed on said recipient computer,

said viewer applet being arranged to decode control information appended to the electronic mail wrapper, search for sender-identity and message-origination fields in said wrapper and control, based on input to said message origination software, a manner in which [an] information items in said selected fields in [an electronic mail] said wrapper [associated with the electronic mail message is] are presented to a recipient of the message, said control including selection of which of said information items are to be [present] presented, and control of coupling of the information and the message.

14. (Amended) A method of controlling an electronic mail message transmitted over a network, comprising the steps of:

after transmission of the electronic mail message over the network, identifying and selecting information in a message wrapper associated with the electronic mail message; and

encrypting said electronic mail message so that only said selected information in said associated message wrapper can be viewed with the message when the electronic mail message is decrypted using a viewer applet installed on a recipient computer.

18. (Amended) A method as claimed in claim 15, wherein said viewer applet is required to establish communications with the central server periodically in order to ensure that [the] a clock used by the viewer applet is functioning properly.

23. (Amended) A method of controlling an electronic mail message as claimed in claim [21] 22, further comprising the steps of encrypting said electronic mail message is carried out by said central electronic mail server using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

24. (Amended) A method of controlling an electronic mail message as claimed in claim [21] 22, further comprising the steps of causing said viewer applet to request forwarding of said electronic mail message stored on said central mail server to a second recipient computer, encrypting said electronic mail message using a public key of a copy of said viewer applet installed on said second recipient computer, and sending said stripped electronic message to said second recipient computer for storage in a memory of the second recipient computer.

25. (Amended) A method of developing mailing lists, comprising the steps of:

sending an electronic mail message to an initial list of recipients;

requiring that [forwarded] versions of said electronic mail message that are forwarded to first additional recipients by said initial recipients be routed through at least one central mail server;

requiring that versions of said electronic mail message that are forwarded to second additional recipients by said first additional recipients be routed through said at least one central mail server;

tracking all transactions involving said electronic mail message, including transactions by said original recipients, said first additional recipients, and said second additional recipients; and

using a record of at least a portion of said transactions to expand said electronic mailing list.

26. (Amended) A method as claimed in claim [24] 25, further comprising the steps of: before initial transmission of said message, attaching handling limitations to said message; and

encrypting said message so that it can only be viewed by a viewer applet supplied by said central server.

27. (Amended) A method as claimed in claim [24] 25, further comprising the steps of: before transmission of the electronic mail message over an open network, attaching to the message a date, time, or event, the occurrence of which will cause said electronic mail message and all designated incarnations thereof to expire; and encrypting said electronic mail message so that it can only be viewed before the occurrence of said time, date, or even using a viewer applet installed on a recipient computer.

28. (Amended) A method as claimed in claim [24] 25, wherein said record includes all addresses to which said message has been forwarded.

29. (Amended) A method as claimed in claim [24] 25, wherein said record includes a subset of the addresses to which said message has been forwarded.

30. (Amended) A method as claimed in claim [24] 25, further comprising the step of selling said expanded list.